UNIVERSIDAD DE BUENOS AIRES

FACULTAD DE INGENIERÍA

CARRERA DE ESPECIALIZACIÓN EN SISTEMAS EMBEBIDOS

MEMORIA DEL TRABAJO FINAL

Módulo de conectividad WiFi/Bluetooth para electrodoméstico

Autor:
Ing. Matías Nicolás Brignone

Director:
Esp. Ing. Diego Fernández (FIUBA)

Jurados:
Mg. Ing. Gonzalo Sánchez (FIUBA, FAA)
Esp. Ing. Matías Álvarez (FIUBA)
Esp. Ing. Santiago Germino (FIUBA)

Este trabajo fue realizado en la ciudad de Córdoba, entre marzo de 2019 y abril de 2020.

Resumen

En la presente memoria se describe el desarrollo de un módulo que permite dotar de conectividad WiFi y Bluetooth a un electrodoméstico, a los fines de permitir su manejo remoto por parte del usuario final. También permite la recopilación de información de uso y estado por parte del fabricante del electrodoméstico. A los fines de agilizar el desarrollo, el electrodoméstico a controlar se emula utilizando un microcontrolador con el cual se comunica el módulo.

Para desarrollar el trabajo, se utilizó un sistema operativo de tiempo real, diferentes protocolos de comunicación en distintas capas (WiFi/Bluetooth para la capa física, HTTPS/MQTT para la capa de aplicación, entre otros), sistemas de control de versiones y herramientas de gestión de proyectos.

Agradecimientos

A mi familia, por su constante apoyo.

A mis amigos y colegas, por acompañarme en este camino.

Índice general

Índice de figuras

Índice de Tablas

Dedicado a mi familia.

Capítulo 1

Introducción General

En este capítulo se realiza una introducción al concepto de Internet de las Cosas, se describe la motivación del trabajo realizado y se presentan los objetivos y el alcance del mismo.

1.1. Internet de las Cosas

Desde la aparición de internet a finales del siglo pasado, ha quedado demostrado continuamente lo increíblemente útil que es contar con un dispositivo capaz de conectarse a la red. Los beneficios de que una computadora o un teléfono inteligente puedan conectarse a internet son evidentes, pero esos beneficios también se encuentran presentes al conectar cualquier otro objeto a internet, y es allí donde surge el concepto de Internet de las Cosas (IoT, por sus siglas en inglés correspondientes a *Internet of Things*).

El Internet de las Cosas consiste básicamente en extender el potencial de internet y la conectividad más allá de las computadoras y celulares, incorporando a todos los objetos (cosas) de la vida cotidiana y que se encuentran presentes en el entorno de una persona, permitiendo la comunicación e interacción entre sí, como así también un monitoreo y control en forma remota.

El concepto de «cosa» es sumamente amplio, ya que contempla desde lámparas, cerraduras y termostatos en el hogar, hasta maquinaria industrial y sistemas de riego para agricultura, pasando por vehículos autónomos, sistemas de iluminación y sensores para estacionamiento público en una ciudad. El objeto conectado incluso puede ser una persona con un monitor cardíaco o un animal de granja con un chip. Gracias a la existencia de sensores y microcontroladores cada vez más potentes, más pequeños y de menor costo, es posible lograr que prácticamente cualquier dispositivo forme parte del ecosistema IoT.

Los beneficios que el Internet de las Cosas ofrece son innumerables, tanto a empresas como a personas individuales. Desde un punto de vista económico, le da la posibilidad a las empresas de conocer y monitorear mejor sus procesos, haciéndolos más eficientes, permitiendo a su vez mejores tomas de decisiones y acciones como mantenimiento predictivo de maquinaria, lo que en definitiva se termina traduciendo en un ahorro de dinero y tiempo para la organización. Con respecto a un individuo particular, el IoT le permite mejorar su calidad de vida y su comodidad en el día a día con automatizaciones en el hogar (domótica), como así también beneficios a la salud con, por ejemplo, implantes inteligentes que permiten un cuidadoso monitoreo.

Las empresas, las personas y el mercado en general hace ya varios años que se han dado cuenta de la importancia del Internet de las Cosas, siendo prueba de ello la gran cantidad de dispositivos conectados que existen, y las proyecciones que indican que estos números seguirán aumentando notablemente. En 2017 ya había 27 mil millones de dispositivos IoT conectados, cifra que aumentará a un ritmo de un 12 % anual hasta llegar a 125 mil millones para 2030 [1]. Por otra parte, en la figura 1.1 se puede observar cómo el mercado mundial del Internet de las Cosas ya maneja cantidades de dinero superiores a los USD 200.000.000.000 (200 mil millones de dólares estadounidenses), y cómo esa cifra aumentará sustancialmente a lo largo de los próximos años [2], lo cual supone una enorme oportunidad de negocio para muchas empresas.

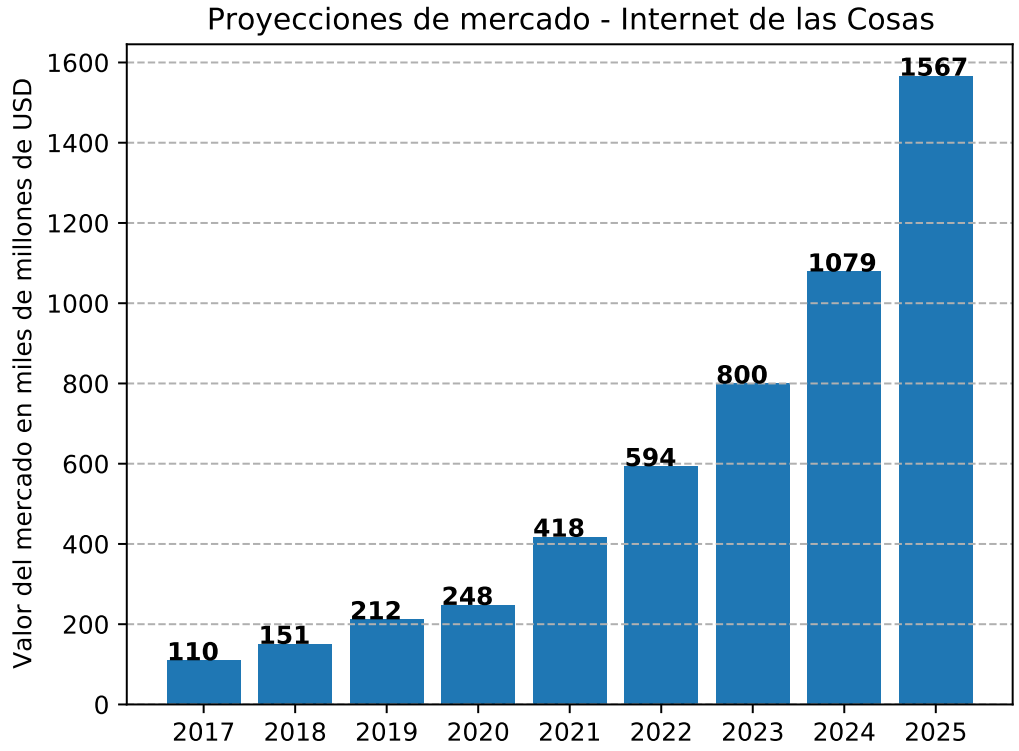

FIGURA 1.1: Proyecciones del valor de mercado a nivel mundial del Internet de las Cosas.[1]

Por último, un punto que a menudo es pasado por alto al momento de hablar de Internet de las Cosas, son todos los problemas asociados a la seguridad y a la privacidad. Tener un mayor número de dispositivos conectados, muchos de los cuales recolectan información sumamente sensible, expande la superficie de ataque considerablemente, haciendo que tanto empresas como personas estén más vulnerables frente a posibles *hackers*. Existen incontables ejemplos de vulnerabilidades en dispositivos IoT que salieron a la luz, como una gigantesca *botnet* formada por dispositivos IoT [3], televisores inteligentes que espían conversaciones privadas [4], e incluso ataques dirigidos a dispositivos conectados en entornos industriales [5]. Estos hechos ocurren principalmente porque la seguridad y la privacidad a menudo son vistos como costos extras en los que no vale la pena incurrir, o incluso en ocasiones la propia empresa utiliza de manera poco ética

[1]Gráfico replicado en base al que se muestra en https://www.statista.com/statistics/976313/global-iot-market-size/.

esos agujeros de seguridad para obtener datos de los usuarios y sacar algún tipo de provecho económico a partir de ellos.

Las consecuencias de una falla de seguridad en un dispositivo IoT pueden ser muy graves, por lo que al momento de desarrollar una solución en el segmento del Internet de las Cosas, los aspectos de seguridad deben ser tenidos en consideración desde un principio, aún cuando ello implique desarrollar un producto más costoso o complejo.

1.2. Estado del arte

En la actualidad, existe una enorme cantidad de dispositivos conectados que pertenecen a muy diversos ámbitos, por lo que resultaría poco práctico brindar un panorama general del estado del arte en todos ellos. Por lo tanto, el foco estará en aquellos productos que ofrezcan soluciones orientadas a dispositivos que ya cuentan con cierto nivel de "inteligencia" (como maquinaria industrial/agrícola o artefactos del hogar), a los fines de dotarlos de conectividad y de todo un entorno que permita procesar y analizar los datos generados por ellos.

Por un lado, existen numerosas plataformas que solamente ofrecen la etapa de procesamiento, análisis y visualización de datos. Estas plataformas asumen que el cliente cuenta con el hardware necesario para enviarles la información relevante, y ellas se encargan de analizarla y presentarla de manera conveniente mediante tableros o *dashboards*, que le permiten al usuario ver el estado de los dispositivos y actuar sobre ellos. La mayoría de estas plataformas cuentan con características similares tales como administración de dispositivos, visualización de datos y soporte a múltiples protocolos de comunicación. Algunos ejemplos de esta clase de plataformas son ThingBoard [6], Thinger [7] y Ubidots [8], además de los servicios específicamente orientados a IoT de Amazon Web Services, de Google Cloud Platform y de Microsoft Azure.

Por otra parte, existen también plataformas de hardware que ofrecen soluciones genéricas de conectividad, junto con plataformas para analizar y visualizar los datos obtenidos, con características similares a las mencionadas anteriormente.

En este último segmento hay diferentes grados de especialización. Por ejemplo, existen empresas que ofrecen soluciones orientadas exclusivamente al ámbito industrial, como ThingWorx de la empresa PTC [9], mientras que otras brindan soluciones más genéricas con una plataforma de hardware y un entorno de análisis y visualización, como el caso de Particle (figura 1.2 [10].)

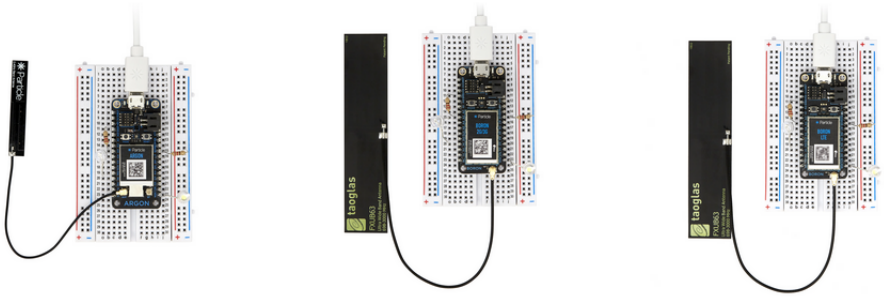

FIGURA 1.2: Plataformas de hardware ofrecidas por Particle.[2]

1.3. Motivación

Un sector fundamental en el ámbito del Internet de las Cosas es el de la domótica, entendiendo por domótica al conjunto de tecnologías que permite el control y la automatización inteligente de una vivienda, a los fines de lograr una gestión eficiente de la misma con mayor comodidad y seguridad para quienes la habitan [11].

A su vez, dentro de la domótica, un campo de especial interés es el de los electrodomésticos inteligentes (o *smart appliances*), tales como televisores, heladeras, hornos, lavarropas o microondas.

Una característica primordial de un electrodoméstico inteligente es su capacidad de estar conectado y ser manejado o accedido de forma remota, ya sea mediante una plataforma web, una aplicación en el celular, comandos de voz o cualquier otro medio. Esta capacidad brinda grandes ventajas con respecto a un artefacto convencional, ya que ofrece no solamente una mayor comodidad al momento de usarlo, sino que también permite programar acciones (como preparar un café a una determinada hora) y ahorrar energía al hacer más eficiente su uso.

Actualmente existen ya en el mercado numerosos ejemplos de electrodomésticos inteligentes que permiten llevar a cabo diferentes acciones:

- Encender el horno mediante un comando de voz, integrándose incluso con los asistentes de voz más comunes.
- Consultar el contenido de la heladera mediante una aplicación en el celular.
- Recibir una notificación cuando el ciclo de lavado del lavarropas finaliza.
- Diagnosticar automáticamente la causa de una falla.

Gracias a las ventajas que ofrecen, la demanda de electrodomésticos inteligentes es cada vez más mayor, por lo que aquellas empresas o fabricantes que no se modernicen y comiencen a incorporar características *smart* a sus dispositivos, se encontrarán en clara desventaja al competir en el mercado con aquellas que sí lo hagan.

Como se puede apreciar en la sección 1.2, existen ya en el mercado numerosas soluciones orientadas al Internet de las Cosas, cada una ofreciendo diferentes características y cubriendo diferentes mercados. Dentro de las soluciones que ofrecen una plataforma tanto de hardware como de software, no existe un sector consolidado que esté orientado a dotar de conectividad a electrodomésticos en el hogar, y es allí donde surge la importancia del presente trabajo. Lo que se busca es cubrir justamente ese sector y ofrecer una solución personalizada a los fabricantes para que puedan lograr que los electrodomésticos que ya fabrican se conviertan en electrodomésticos inteligentes.

[2]Imagen extraída de https://store.particle.io/pages/prototyping-hardware.

1.4. Objetivos y alcance

1.4.1. Objetivos generales

El objetivo general del presente trabajo es el diseño e implementación de un módulo capaz de dotar de conectividad WiFi y Bluetooth a un electrodoméstico convencional. Para ello, el módulo debe tener la capacidad de comunicarse con la placa del propio equipo y de recibir/enviar información a un servidor en la nube, a los fines de permitirle al usuario final un manejo remoto del aparato y conocer su estado, como así también enviar información de uso al fabricante.

El módulo no está destinado directamente al usuario final que haría uso del electrodoméstico, sino a empresas o fabricantes que busquen incorporar características inteligentes a sus electrodomésticos.

A grandes rasgos, desde el punto de vista del usuario final, se debe permitir:

- Enviar por WiFi o Bluetooth un comando al electrodoméstico que dispare una acción en el mismo, como iniciar la cocción en un horno o el lavado en un lavarropas.
- Conocer el estado del electrodoméstico mediante la recepción de información por WiFi o Bluetooth.

Por otra parte, desde el punto de vista del fabricante del electrodoméstico, se debe permitir:

- Recibir y almacenar información acerca del estado de todos los dispositivos (si están o o no conectados, y en qué estado de ejecución se encuentran).
- Analizar y visualizar de manera conveniente la información de estado de los dispositivos a lo largo del tiempo.

1.4.2. Alcance

El presente trabajo incluye los siguientes aspectos:

1. Análisis, investigación y elección del hardware a utilizar en el módulo.
2. Implementación del firmware del sistema.
3. Comunicación con un microcontrolador que emule el comportamiento del electrodoméstico.
4. Desarrollo de una interfaz web mediante una plataforma ya existente, que permita enviarle comandos al electrodoméstico emulado.
5. Implementación de un entorno en la nube que permita analizar y visualizar los datos de los diferentes electrodomésticos conectados.

Es de especial importancia el punto 3 de la lista, en el que se define explícitamente que, a los fines de agilizar considerablemente el tiempo de desarrollo del trabajo, el prototipo no se utilizará en un electrodoméstico real. La interacción con el electrodoméstico se emula mediante la comunicación con otro microcontrolador, que actúa como la placa de control del mismo, por lo que imita su comportamiento y sus respuestas ante diferentes estímulos.

En línea con el párrafo anterior, el presente trabajo NO incluye lo siguiente:

1. Integración del prototipo a diferentes electrodomésticos/marcas con distintos tipos de comunicación serie y funcionalidades.
2. Desarrollo de una aplicación móvil desde la cual interactuar por Bluetooth con el módulo.
3. Diseño y fabricación de un circuito impreso. Para el trabajo se utiliza una placa de prototipo ya existente que incluye el hardware seleccionado.

Capítulo 2

Introducción Específica

Párrafo introductorio.

2.1. Funcionamiento general del sistema

2.2. WiFi y Bluetooth Low Energy

2.3. Protocolos HTTP/S y MQTT

2.4. Requerimientos

2.5. Planificación

Capítulo 3

Diseño e Implementación

Párrafo introductorio.

3.1. Entorno de desarrollo

3.2. Firmware

3.2.1. Arquitectura MQTT

3.2.2. Tareas implementadas

3.3. Interfaz de usuario

3.4. Integración con Google Cloud Platform

Capítulo 4

Ensayos y Resultados

Párrafo introductorio.

4.1. Pruebas funcionales

4.1.1. Comunicación WiFi

Servidor web

4.1.2. Comunicación BLE

4.1.3. Comunicación serie con electrodoméstico

4.2. Integración del sistema

4.2.1. Visualización de datos en Google Cloud Platform

Capítulo 5

Conclusiones

5.1. Conclusiones generales

5.2. Próximos pasos

Bibliografía

[1] IHS Markit. *The Internet of Things: a movement, not a market*. 2017.

[2] Statista. *Forecast end-user spending on IoT solutions worldwide from 2017 to 2025*. https://www.statista.com/statistics/976313/global-iot-market-size/. 2017. (Visitado 14-03-2020).

[3] Cloudflare. *What is the Mirai Botnet?* https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/. (Visitado 15-03-2020).

[4] Zack Whittaker. *CIA, MI5 hacked smart TVs to eavesdrop on private conversations*. https://www.zdnet.com/article/how-cia-mi5-hacked-your-smart-tv-to-spy-on-you/. 2017. (Visitado 15-03-2020).

[5] Danny Palmer. *Ransomware, snooping and attempted shutdowns: see what hackers did to these systems left unprotected online*. https://www.zdnet.com/article/ransomware-snooping-and-attempted-shutdowns-the-state-of-this-honeypot-shows-what-hackers-do-to-systems-left-unprotected-online/. 2020. (Visitado 15-03-2020).

[6] https://thingsboard.io/. (Visitado 18-03-2020).

[7] https://thinger.io/. (Visitado 18-03-2020).

[8] https://ubidots.com/. (Visitado 18-03-2020).

[9] *ThingWorx*. https://www.ptc.com/-/media/Files/PDFs/IoT/ThingWorx-Connect-Product-Brief.pdf. (Visitado 18-03-2020).

[10] https://www.particle.io/. (Visitado 18-03-2020).

[11] Asociación Española de Domótica e Inmótica. *Qué es Domótica*. http://www.cedom.es/sobre-domotica/que-es-domotica. (Visitado 17-03-2020).